Revista Logos Ciencia & Tecnología, 16 (1) 83-107 | Enero-abril, 2024
https://revistalogos.policia.edu.co:8443/index.php/rlct

Artículo de investigación

Revista Logos Ciencia & Tecnología
ISSN-L 2145-549X
ISSN 2422-4200 (en línea)

Cooperación internacional policial ante amenazas cibernéticas en Colombia: *Modalidad Business Email Compromise*

International police cooperation on cyber threats in Colombia: Business Email Compromise Modality

Cooperação internacional para a aplicação da lei sobre ameaças cibernéticas na Colômbia: Modalidade de Comprometimento de E-Mail Comercial

Luis Evelio Castillo Pulido [a,*] | Juan Felipe Jiménez Acosta [b]

a https://orcid.org/0000-0002-5548-8424 Universidad de la Salle, Colombia

b Escuela de Postgrados de Policía Miguel Antonio Lleras Pizarro, Bogotá, Colombia

- Fecha de recepción: 2023-12-07
- Fecha concepto de evaluación: 2024-01-10
- Fecha de aprobación: 2024-01-25
https://doi.org/10.22335/rlct.v16i1.1877

Para citar este artículo/To reference this article/Para citar este artigo: Castillo Pulido, L. E., & Jiménez Acosta, J. F. (2024). Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. *Revista Logos Ciencia & Tecnología, 16(*1), 83-107. https://doi.org/10.22335/rlct.v16i1.1877

RESUMEN

Esta investigación tiene como objetivo identificar un modelo de cooperación policial internacional aplicable a las diferentes manifestaciones de las amenazas cibernéticas en Colombia: robo por medios informáticos, a través de la industria *Business Email Compromise* (BEC). Se ha seguido un enfoque interpretativo, que permite entender el panorama cibernético desde la perspectiva de especialistas académicos, considerando sus creencias y actitudes. Además, se adoptó una metodología mixta que integra enfoques cualitativos y cuantitativos, lo que facilita la triangulación de datos provenientes tanto del trabajo de campo, como de análisis teóricos y descriptivos. Los hallazgos clave sugieren que un patrón BEC internacional está relacionado con facturas falsas, bienes raíces y fraude de directores ejecutivos, así como compromisos de correo electrónico doméstico. Los actores más afectados son los organismos multilaterales, las empresas privadas y públicas, respectivamente; se ha relacionado con el tráfico de armas, la trata de personas, la explotación sexual, el tráfico de drogas y el tráfico de órganos.

Palabras clave: Compromiso de correo empresarial (BEC), ciberseguridad, cooperación internacional, ciberdelincuencia, amenazas cibernéticas.

ABSTRACT

The objective of this research was to identify a model of international police cooperation applicable to the different manifestations of cyber threats in Colombia: theft by means of computer, through the Business Email Compromise (BEC) industry; its development has been achieved

*Autor de correspondencia. Correo electrónico: luis96617@gmail.com

through an interpretive research model that provides an understanding of beliefs and attitudes that make it possible to comprehend the world from the perspective of academic experts; additionally, a mixed approach through which synergies are established and qualitative and quantitative methodologies are complemented; research methods that simultaneously allow for the triangulation of information obtained from field work and theoretical and descriptive/phenomenological studies; Key findings suggest that an international BEC pattern is linked to false invoices, real estate and CEO fraud, as well as domestic email compromises. the most affected actors are multilateral organisations, private and public companies, respectively; It has been linked to arms trafficking, human trafficking, sexual exploitation, drug trafficking, and organ trafficking.

Keywords: Business Email Compromise (BEC), cyberthreat, cyberspace, multistakeholders, International Police Cooperation Model.

RESUMO

O objetivo desta pesquisa foi identificar um modelo de cooperação policial internacional aplicável às diferentes manifestações de ameaças cibernéticas na Colômbia: roubo por meio de computador, através da indústria de Business Email Compromise (BEC); seu desenvolvimento foi alcançado por meio de um modelo de pesquisa interpretativa que fornece uma compreensão de crenças e atitudes que permitem entender o mundo a partir da perspectiva de especialistas acadêmicos; adicionalmente, uma abordagem mista através da qual se estabelecem sinergias e se complementam metodologias qualitativas e quantitativas; métodos de investigação que permitam simultaneamente a triangulação da informação obtida no trabalho de campo e em estudos teóricos e descritivos/fenomenológicos; As principais descobertas sugerem que um padrão internacional de BEC está vinculado a faturas falsas, fraudes imobiliárias e de CEOs, bem como comprometimentos domésticos de e-mail. os atores mais afetados são organizações multilaterais, empresas privadas e públicas, respectivamente; Tem sido associado ao tráfico de armas, tráfico de seres humanos, exploração sexual, tráfico de drogas e tráfico de órgãos.

Palavras chave: Comprometimento de email empresarial (BEC), cibersegurança, cooperação internacional, cibercrime, ameaças cibernéticas.

Introducción

Los cibercrímenes presentan características particulares que abarcan la naturaleza de la acción, el sujeto involucrado, los resultados obtenidos y la imputación correspondiente. Estas características demuestran que la teoría del delito requiere una complementación o incluso una reevaluación en algunos aspectos, con el fin de explicar y aplicar de manera adecuada estas fenomenologías digitales que se producen habitualmente en entornos virtuales y deslocalizados, donde cada vez se observa más una intervención menos directa por parte del ser humano (Posada, 2017).

Desde una perspectiva histórica, los registros existentes sobre los ataques cibernéticos indican que, en el mundo, las manifestaciones de este fenómeno datan desde 1999. Un ejemplo relevante del crimen informático tuvo lugar en la NASA, cuando Jonathan Joseph James accedió de manera ilícita a 13 ordenadores, sustrayendo un software cuyo valor se estima en 1.7 millones de dólares. Este incidente provocó el cierre de la NASA durante 21 días, generando costos de reparación y pérdidas por un total de 41 000 dólares. Es importante destacar que dicho software controlaba elementos críticos de supervivencia en la Estación Espacial Internacional (Álvarez, 2019).

A este evento se suma el incidente ocurrido en el 2015 en Ucrania, cuando una red eléctrica sufrió un apagón de seis horas, debido a la infiltración en tres empresas distribuidoras de energía y la posterior interrupción temporal de los generadores en tres regiones del país. Según las compañías de seguridad estadounidenses, estos ataques fueron llevados a cabo por el gobierno ruso (DW, 2019).

Otro acontecimiento de gran relevancia tuvo lugar con el surgimiento del *ransomware* conocido como WannaCry, el cual infectó aproximadamente a 300 000 computadoras en 150 países en mayo de 2017. Este *software* malicioso se encargaba de cifrar los archivos de los usuarios y exigía un rescate de cientos

de dólares a cambio de las claves necesarias para descifrar los archivos. Este ataque afectó a la sede de Telefónica en Madrid, al Sistema de Salud Británico y al Ministerio del Interior ruso. Asimismo, la compañía FedEx informó haber sufrido pérdidas de cientos de millones de dólares como consecuencia de este ataque. Tanto Estados Unidos como Reino Unido acusaron a Corea del Norte de ser el responsable de este incidente, aunque Pyongyang negó tales acusaciones y las catalogó como una "grave provocación política" (Oliveira, 2017).

Además, es necesario destacar un evento significativo en el espectro de la ciberseguridad que tuvo lugar en el 2019, concerniente al Bundestag alemán. En este episodio, las entidades políticas representadas en la Cámara Legislativa alemana, con la notable excepción de la formación de derecha Alternativa para Alemania (AFD, por sus siglas en alemán), fueron objeto de un ataque cibernético. A lo largo de esta incursión digital, los perpetradores consiguieron infiltrarse y obtener acceso a activos informacionales de carácter sensible, incluyendo registros financieros, documentos de identificación y correspondencia privada entre los parlamentarios. Después, esta información fue ilegítimamente divulgada en plataformas en línea. Destaca entre la información comprometida, detalles personales de la canciller Ángela Merkel, tales como su número de fax y su dirección de correo electrónico, así como varios intercambios de correspondencia (Otero, 2019).

Ahora bien, en el ámbito nacional, según el Centro Cibernético de la Policía Nacional, las amenazas cibernéticas que han afectado a Colombia han estado mayormente relacionadas con delitos de hurto, los cuales han sido considerados de alto impacto desde el 2018, debido al incremento en el número de denuncias relacionadas con este tipo de delito, las cuales ascendieron a un total de 12014 casos (Ramírez, 2019).

Es importante destacar que una de las manifestaciones de este problema se ha observado en el ámbito de los fraudes financieros, el acceso ilícito a contraseñas para el robo de datos, así como las falsificaciones llevadas a cabo a través de dispositivos electrónicos. De acuerdo con el informe titulado "El rompecabezas imposible de la ciberseguridad", el 53% de los casos de ciberataques fueron perpetrados por medio del empleo de correos electrónicos, en los cuales prevalece la técnica de suplantación de identidad para obtener información confidencial como contraseñas o números de tarjetas de crédito (Colprensa, 2019).

En cuanto a los sectores empresariales nacionales, se constató que la mayoría de los ciberataques tuvieron lugar en los servidores (41.5%), seguidos de la red (35.4%), los puntos finales (16.5%) y los dispositivos móviles (6.7%). No obstante, resulta preocupante que el 26.8% de los gerentes de TI (tecnologías de la información) desconozca cómo se produjo el ciberataque de mayor impacto experimentado por su organización, mientras que el 78.7% ignora cuánto tiempo estuvo antes de detectarlo (Virtualpro, 2019).

Estos ejemplos ilustran la creciente sofisticación y el alcance global de los ciberataques, así como las consecuencias perjudiciales que pueden acarrear en diversos ámbitos, como el sector empresarial, la seguridad nacional y la infraestructura crítica. Es fundamental destacar la necesidad de abordar estos desafíos desde una perspectiva académica y multidisciplinaria para desarrollar estrategias efectivas de prevención, detección y respuesta ante los cibercrímenes.

De tal manera, es posible ver que resultaba imperativo analizar y comprender las características específicas de estos delitos en términos de su naturaleza, los actores involucrados, los métodos utilizados y las consecuencias resultantes. Asimismo, ampliar el corpus teórico existente en el campo del derecho penal y adaptarlo a las complejidades y dinámicas propias del entorno digital.

En este sentido, es necesaria una revisión y actualización de la teoría del delito para abordar adecuadamente los aspectos singulares que se presentan en el ciberdelito. La intervención humana cada vez menos directa, la realidad virtual y remota, y la interconexión global de sistemas y dispositivos plantean desafíos únicos que requieren nuevas herramientas conceptuales y legales. Dicho lo anterior, la promoción de la cooperación internacional y la cooperación entre los sectores público y pri-

vado es fundamental para combatir eficazmente los ciberataques. Las partes interesadas, tanto gubernamental como corporativa, deben compartir información, mejores prácticas y recursos para mejorar la ciberseguridad a escala global.

Así, en consonancia con lo expuesto, el ciberdelito representa una realidad compleja y en constante evolución que requiere un riguroso enfoque académico y una respuesta global. El estudio y comprensión de estos fenómenos delictivos digitales requiere una teoría criminal extensa, un vocabulario preciso y coherente, así como un análisis detallado de los casos y sus contextos. Solo un enfoque multidisciplinario y colaborativo efectivo puede enfrentar los desafíos que plantean los ataques cibernéticos en la sociedad contemporánea.

Dicho con mayor énfasis, la seguridad pública y la comprensión de su importancia en el ámbito de la seguridad nacional y su repercusión en el escenario internacional, resulta de vital trascendencia adoptar las mejores prácticas de modelos exitosos de seguridad. Estas prácticas permitirán la construcción de estrategias centradas en la prevención de las "amenazas cibernéticas", las cuales afectan directamente tanto al sector público como al privado y a la sociedad civil. Ante este panorama y considerando las nuevas amenazas a la seguridad pública, resulta crucial hacer referencia a los documentos del "Consejo Nacional de Política Económica y Social", elaborados mediante la colaboración de las autoridades político-administrativas más representativas del Estado. En consecuencia, como se afirma en los documentos Conpes de 2001, podemos afirmar que la iniciativa se centra en "generar directrices de política en ciberseguridad y ciberdefensa con el objetivo de desarrollar una estrategia nacional que contrarreste el aumento de las amenazas informáticas que afectan significativamente al país".

Este estudio asume la seguridad pública como su objeto. En este contexto, los delitos cibernéticos emergen como una amenaza inminente para la seguridad estatal. Cabe resaltar que la doctrina y la jurisprudencia favorecen la teoría de la ubicuidad, la cual considera relevantes tanto el lugar de comisión del acto como donde ocurre el perjuicio (Rayon et al., 2014). En este orden de ideas, la sociedad desempeña un rol crucial como uno de los agentes más influyentes en la confrontación de las amenazas cibernéticas. Conforme a lo señalado, tales amenazas afectan significativamente los sectores público, privado y civil (Navarro Asencio et al., 2017).

La presente investigación analiza la seguridad pública como un componente crítico frente a las amenazas cibernéticas, adoptando un prisma analítico fundamentado en teorías de ciberseguridad de amplio reconocimiento. Internacionalmente, se destaca la teoría del "neorrealismo", que postula la anarquía sistémica y la competencia por la seguridad en el ciberespacio, así como la "interdependencia compleja", que argumenta a favor de la cooperación estatal y no estatal en el ámbito digital. A escala nacional, se consideran marcos teóricos que subrayan la importancia de la construcción de capacidades estatales y políticas de ciberseguridad, resaltando la necesidad de colaboración multiactor para fortalecer la infraestructura cibernética de Colombia. Con base en el análisis de estas teorías, se puede inferir que Colombia actualmente enfrenta desafíos significativos en anticipar y mitigar las amenazas cibernéticas, lo que resalta la urgencia de desarrollar estrategias integrales que aborden la seguridad cibernética como una prioridad nacional. Este enfoque teórico proporciona un marco para entender y abordar las complejidades del ciberdelito y sus implicaciones en la seguridad pública del país.

Es destacable que el problema central se fundamenta en "la falta de capacidad actual del Estado para enfrentar las amenazas cibernéticas", situación abordada por el documento Conpes (Política Nacional de Confianza y Seguridad Digital) 3995 de 2020. Este documento estratégico señala la imperiosa necesidad de actualizar y fortalecer las políticas de seguridad digital del país, en respuesta al incremento y la complejidad de los ciberdelitos, que han escalado en 72% en costos para los negocios entre el 2014 y 2019. Por tanto, se

enfatiza la importancia de establecer medidas para expandir la confianza digital y asegurar un entorno socioeconómico seguro y confiable, lo cual es vital para mantener a Colombia competitiva en el panorama digital global (Conpes, 2020).

En este sentido, es crucial reconocer que la ciberseguridad se ha convertido en un desafío cada vez más apremiante en el contexto actual. A medida que la sociedad depende cada vez más de las tecnologías de la información y la comunicación, también se incrementa la vulnerabilidad a los ciberataques y a la explotación de las redes digitales. La rápida evolución de las amenazas cibernéticas plantea la necesidad de adoptar medidas eficaces para salvaguardar la seguridad y la integridad de los sistemas informáticos y proteger la información sensible.

En este contexto, resulta evidente la importancia de llevar a cabo investigaciones que permitan comprender exhaustivamente las dimensiones y complejidades de las amenazas cibernéticas y contribuyan al diseño e implementación de políticas públicas efectivas en materia de ciberseguridad. Es necesario desarrollar estrategias nacionales que promuevan la cooperación interinstitucional, la capacitación especializada y la concientización de la sociedad en general sobre los riesgos y las buenas prácticas en el ámbito digital.

Además, es fundamental establecer marcos legales y normativos sólidos que permitan sancionar de manera adecuada los delitos cibernéticos y brinden un marco de protección legal para las víctimas. La colaboración internacional también desempeña un papel fundamental en la lucha contra las amenazas cibernéticas, ya que estas trascienden las fronteras nacionales y requieren una respuesta coordinada y cooperativa a nivel global.

De suerte que la prevención y mitigación de las amenazas cibernéticas se han convertido en una prioridad tanto nacional como internacional. Es necesario fortalecer la capacidad del Estado para hacer frente a estos desafíos, a través de la formulación de estrategias integrales que involucren a todos los actores relevantes. La investigación en este campo desempeña un papel fundamental para comprender y abordar de manera efectiva las amenazas cibernéticas, garantizando así la seguridad pública en el entorno digital. Solo a través de un enfoque multidisciplinario, el intercambio de conocimientos y la colaboración, será posible hacer frente a este creciente fenómeno y salvaguardar los sistemas informáticos y la confianza en el entorno digital.

Frente a lo anterior y en el marco de la seguridad pública, conscientes de la importancia de abordar las amenazas cibernéticas en el país, resulta fundamental caracterizar la modalidad de hurto por medios informáticos conocida como *Business Email Compromise* (BEC). Esta forma de delito cibernético ha ganado presencia en Colombia y requiere de un análisis exhaustivo para comprender su alcance y sus implicaciones en la seguridad pública. Además, es crucial identificar los instrumentos de cooperación internacional policial suscritos por Colombia en los últimos tres años con relación a esta manifestación delictiva. Estos acuerdos y convenios de cooperación brindan oportunidades para fortalecer la capacidad de respuesta y el intercambio de información entre los organismos encargados de combatir el BEC. Por último, es necesario definir las acciones específicas que la Policía Nacional de Colombia debe implementar en materia de cooperación internacional policial para enfrentar de manera efectiva a las manifestaciones del delito *Business Email Compromise*. Esto implicaría establecer canales de comunicación eficientes, promover la capacitación especializada y fomentar la colaboración con otras agencias policiales en el escenario internacional. Así, el norte de la investigación consistió en dar respuesta a la cuestión: ¿cuál es el modelo de cooperación internacional policial ante la materialización de las amenazas cibernéticas en Colombia como el hurto por medios informáticos, en la modalidad BEC (Business Email Compromise)?

Dicho de otra forma, se vuelve crucial entender la magnitud y las intrincadas dinámicas del delito cibernético de hurto mediante medios informáticos, sobre todo bajo la modalidad del Business Email Compromise (BEC). Esta categoría de crimen cibernético, que facilita la obtención ilícita de información y la usurpación de identidades a través del engaño en

comunicaciones electrónicas, representa un reto significativo para la seguridad cibernética. Ante esta realidad, es esencial dominar los conceptos claves relacionados.

Con respecto a esto, una perspectiva inicial del término "cooperación internacional" desde un enfoque teórico se encuentra relacionada con las perspectivas ortodoxas del desarrollo. Walt Whitman Rostow, exconsejero de Seguridad Nacional de los Estados Unidos, uno de los principales exponentes en este campo, establece en 1961 que la cooperación internacional abarca distintas etapas de desarrollo. En primer lugar, se encuentra la etapa tradicionalista, donde los recursos necesarios para el crecimiento de un país y su sociedad son escasos. A continuación, surge la etapa de industrialización, en la cual el desarrollo de la industria y la agricultura aportan una dosis de modernidad al Estado, generando un crecimiento económico. Posteriormente, se alcanza la etapa de despegue económico, caracterizada por el incremento en la producción y el crecimiento de los sectores económicos, como la manufactura. Luego, se presenta la etapa de consolidación, donde los avances tecnológicos y la modernización desempeñan un papel fundamental. Por último, se encuentra la etapa de consumo social o de masas, en la cual se busca satisfacer las necesidades básicas de los ciudadanos a través de servicios accesibles (Slater, 1999).

En el ámbito del desarrollo de los derechos humanos, la cooperación internacional emerge de la unión coordinada de esfuerzos, tanto domésticos como globales, llevados a cabo por organizaciones que gestionan situaciones demandantes de inversión, las cuales pueden estar fuera del ámbito regulador estatal o social. Esta forma de colaboración internacional es fundamental para enfrentar desafíos sociales, fungiendo como un medio de equidad y justicia en la gestión y asignación de recursos financieros (Restrepo Silva, 2012, p. 284).

En este contexto, el paradigma neoinstitucionalista ofrece una alternativa a la postura económica clásica al analizar el comportamiento de los Estados desde la perspectiva de las relaciones internacionales y el cambio institucional generado por las acciones humanas, lo cual puede conducir a cambios significativos en aquellos Estados que lo implementan. Según Robert Keohane, existe una mayor cooperación entre Estados que se basa en una adecuada planificación y negociación para lograr acuerdos que beneficien a todas las partes involucradas (Jiménez González, 2003, p. 135).

El delito cibernético conocido como hurto por medios informáticos, en la modalidad BEC (*Business Email Compromise*), representa una amenaza significativa tanto para personas naturales como para entidades jurídicas. Este tipo de delito permite a los cibercriminales obtener información confidencial con el objetivo de suplantar identidades mediante la falsificación de correos electrónicos. Como lo afirma Ceballos López (2019), mediante esta suplantación, los delincuentes logran desviar fondos hacia sus propias cuentas bancarias y también engañan a clientes y proveedores al solicitar envíos de mercancías. La reflexión permite afirmar que este comportamiento delictivo en el ámbito tecnológico no puede ser considerado como parte de otras conductas delictivas diseñadas para proteger bienes físicos o materiales. Por ejemplo, los delitos de hurto o estafa, creados por el legislador para salvaguardar bienes materiales muebles e inmuebles, no pueden abordar de manera adecuada el delito de transferencia no consentida de activos. La razón de esto radica en que este último se centra fundamentalmente en datos inmateriales, como el software, y su procedimiento no implica engañar directamente a una persona ni apoderarse de objetos mediante técnicas de ingeniería social.

Un síntoma de la resistencia ante esta nueva realidad, es considerar el ciberespacio y los sistemas informáticos y telemáticos como simples instrumentos casuales utilizados en la comisión de ciberamenazas. Incluso, estos medios se comparan erróneamente con los delitos computacionales o relacionados con la conexión a la red para el tratamiento de datos, información y sistemas informáticos, que implican la utilización de elementos incorporales. Es importante tener en cuenta que los delitos vinculados al internet, a diferencia de las ciberamenazas, protegen principalmente otros bienes jurídicos, como la intimidad o el patrimonio económico, antes que la seguridad de la información, los datos y los sistemas informáticos, que se protegen de manera indirecta (Posada, 2017).

Ahora bien, un último concepto que es importante no perder de vista, es la cooperación internacional, pues se refiere a la corresponsabilidad que surge a partir del postulado de solidaridad entre naciones, con el propósito de promover el desarrollo y garantizar el respeto de los derechos de los ciudadanos de un país. Asimismo, busca crear condiciones favorables que propicien el bienestar y la valoración de la dignidad humana. En este sentido, la cooperación internacional se materializa mediante la identificación de prioridades, el establecimiento de metas y el desarrollo de estrategias de trabajo conjunto, así como la interacción constante entre las partes involucradas para lograr la sincronización de intereses (Duarte Herrera & González Parias, 2014, p. 118).

Metodología

En el marco metodológico se incluyen los instrumentos utilizados para la recolección de datos cuantitativos y cualitativos. En particular, para la información cualitativa, se llevaron a cabo entrevistas semiestructuradas con expertos en ciberseguridad. Estas entrevistas se validaron mediante un proceso de revisión por pares y pilotos iniciales con profesionales del campo para asegurar su relevancia y precisión. Se establecieron criterios de selección rigurosos para la población y la muestra, optando por un muestreo estratificado que refleje la diversidad y experiencia en la materia. La validación de los resultados cualitativos se efectuó a través de triangulación de datos, corroboración con literatura secundaria y análisis de contenido. Este compendio de estrategias metodológicas posibilita una evaluación integral del modelo de cooperación internacional policial frente a las amenazas cibernéticas en Colombia durante el 2019.

Esta investigación se fundamenta en el paradigma interpretativo, que resulta esencial para entender los conceptos y comparar con otros paradigmas de investigación. Según Pérez Serrano (1994), y refiriéndose a Cook, existen distintos paradigmas que ofrecen perspectivas únicas y complementarias sobre el mundo. Tanto el positivismo como el interpretativismo son fundamentales para una comprensión integral de la realidad (Pérez Serrano, 1994, p. 62).

Esta investigación adopta un enfoque mixto, y reconoce la necesidad de complementar los enfoques cualitativo y cuantitativo para lograr una aproximación más completa al tema de investigación. Esto permite al investigador llevar a cabo la triangulación tanto en la aplicación de instrumentos, como en el análisis de la información recopilada durante el trabajo de campo. Dicha complementariedad resulta fundamental para abordar de manera integral el fenómeno social y los factores que influyen en él, fundamentando así la elección del paradigma interpretativo, en línea con las tres características más relevantes que propone Pérez Serrano (1994).

De este modo, se estableció que el desarrollo de la investigación se fundamentó en un enfoque mixto, combinando la utilización de instrumentos de recolección de datos cuantitativos y cualitativos. En el ámbito cuantitativo, se aplicó un cuestionario estructurado, mientras que en el cualitativo se realizó una entrevista exhaustiva, lo cual permitió obtener información alineada con los objetivos de investigación previamente establecidos (ver en anexos).

En cuanto al diseño de la investigación, se sustentó en el modelo mixto tipo VII, que implicó la simultaneidad en la recopilación y el análisis de datos cuantitativos y cualitativos (Rocco, 2003). Este diseño se eligió para aprovechar las fortalezas de ambos enfoques y obtener una comprensión más completa del fenómeno estudiado.

En términos de organización, se siguió una estrategia secuencial explicativa, tal como planteó Creswell (2008). En esta estrategia, los resultados cualitativos sirvieron como base para explicar los hallazgos cuantitativos, lo que permitió establecer relaciones y generar un conocimiento más profundo del tema.

Respecto al método de investigación, se empleó un enfoque concurrente, mediante el cual se recolectaron datos cualitativos y cuantitativos de manera simultánea y se compararon los resultados en el análisis. En el 2019, se presentó como objetivo principal una propuesta para articular la cooperación internacional policial en la generación de capacidades de respuesta ante las "amenazas cibernéticas" en Colombia.

Además, el método concurrente consideró cuatro aspectos fundamentales para su desarrollo. Primero, se analizaron de manera paralela los datos cualitativos y cuantitativos. Segundo, se realizó un análisis independiente de los resultados obtenidos mediante cada método aplicado. Tercero, una vez finalizada la recolección de datos, se llevó a cabo un análisis integrado basado en los datos cualitativos y cuantitativos recopilados. Por último, se realizaron meta-inferencias basadas en los resultados obtenidos, contribuyendo a un análisis más profundo y enriquecedor (Hernández et al., 2014). En consecuencia, al adoptar un enfoque mixto, se logra la posibilidad de comprender los significados atribuidos al objeto de estudio por parte de los diversos actores y fuentes consultadas. Mediante el estudio de caso, se busca obtener un conocimiento más profundo acorde con las necesidades investigativas.

Con relación a la fase fenomenológica, esta se centra en la exploración de los elementos que explican la realidad circundante del objeto de estudio, mediante la comprensión de los componentes de cada aspecto relevante para la generación de conocimiento pertinente (Aguirre García & Jaramillo Echeverri, 2012). Para llevar a cabo una investigación fenomenológica, es necesario considerar pasos como la preparación de la recolección de datos, su organización, análisis y reducción, así como el resumen de resultados y sus implicaciones (Aguirre García & Jaramillo Echeverri, 2012, p. 64). En el caso presentado, se efectuó una entrevista exhaustiva como instrumento de recolección de datos.

Por otro lado, la fase descriptiva se refiere al estudio minucioso de las características de un fenómeno, sin buscar las causas ni las consecuencias de su configuración. Mediante esta fase, el investigador obtiene una imagen detallada del tema de interés (Bisquerra, 2009). Es importante destacar que la investigación descriptiva permite conocer cada una de las características del tema en estudio, empleando diferentes instrumentos que no son excluyentes entre sí (Bisquerra, 2009, p. 233).

En este contexto, se llevó a cabo una descripción detallada de la amenaza cibernética de hurto por medios informáticos en la modalidad BEC presente en el país. Para ello, se tuvieron en cuenta diversos factores, los cuales se describen en la Tabla 1, con el objetivo de fundamentar la caracterización de dicha amenaza.

Tabla 1

Factores de análisis

No.	Factor	Descripción
1	Información	Comprende los datos de identificación de la persona que suministró la información en el desarrollo de la encuesta.
2	Modalidades	Hace referencia a las formas de presentación más recurrentes del BEC en el país.
3	Técnicas	Tiene relación con el procedimiento que tiene lugar al momento de llevar cada una de las modalidades del BEC en el país.
4	Población objetivo	Establece los segmentos de población que son proclives al recibir la afectación del BEC.
5	Asociación	Hace alusión a las redes con las cuales los grupos criminales que lo aplican establecen relación para facilitar el desarrollo del BEC.
6	Actores ilegales	Se relaciona con los actores ilegales que pueden intervenir en el desarrollo de esta modalidad de delito cibernético.
7	Acciones de defensa	Comprende las actividades adelantadas por el Estado colombiano o de las instituciones o personas para llevar a cabo el BEC.
8	Actores legales	Se relaciona con las instituciones, organizaciones y demás actores que trabajan en pro de fortalecer la ciberseguridad.

Resultados

En este apartado se presentan los resultados obtenidos a partir de la realización de una en-

trevista exhaustiva sobre el fenómeno del Compromiso de Correos Electrónicos Corporativos (BEC, por sus siglas en inglés). Esta entrevista constituye la primera fase del estudio. Posteriormente, se exponen los resultados obtenidos a través de la aplicación de un cuestionario en la segunda fase. Como tercer aspecto, se hace una triangulación de los resultados mediante el análisis concurrente de cada uno de los objetivos específicos establecidos en el marco de esta investigación.

La entrevista realizada a cuatro funcionarios expertos en Business Email Compromise (BEC) reveló información clave. Respecto a la primera pregunta sobre los instrumentos de cooperación internacional implementados por Colombia en los últimos tres años para contrarrestar el BEC, los especialistas coincidieron en que no se han establecido mecanismos específicos dirigidos al cibercrimen y al BEC. No obstante, se destaca la participación de la Policía Nacional en la Joint Cybercrime Action Taskforce (J-CAT) de Europol, como parte de una comisión de servicio permanente en el extranjero, lo cual representa un esfuerzo en la lucha contra dichas amenazas cibernéticas.

En relación con la pregunta, que buscaba identificar los proyectos en curso dentro de los instrumentos de cooperación internacional creados por Colombia en los últimos tres años para abordar las manifestaciones del BEC, los expertos señalaron que Colombia está llevando a cabo gestiones para formar parte del proceso enmarcado en la Convención de Cibercriminalidad. Además, se destacó que las actividades que se desarrollan en la actualidad son principalmente preventivas. Asimismo, se está trabajando en consonancia con un proyecto de Europol llamado Joint Cybercrime Action Taskforce (J-CAT), el cual está enfocado en atender este tipo de amenazas.

Otra de las preguntas indagaba acerca de los programas que se están implementando en el marco de los instrumentos de cooperación internacional, establecidos por Colombia en los últimos tres años para hacer frente a las manifestaciones del BEC. De acuerdo con los expertos, los programas en curso dentro de los instrumentos de cooperación están relacionados con el Centro Europeo de Cibercrimen (EC3) de Europol, el cual proporciona ventajas en el pronóstico de los ataques BEC. Además, se destacaron los programas de capacitación, la adhesión al Convenio de Budapest y el acceso a la plataforma J-CAT para abordar este tipo de amenazas. Estas iniciativas se enfocan actualmente en el desarrollo de investigaciones, soporte técnico y forense, así como en la capacitación. Cabe señalar que los programas no se han concebido como una posible suscripción de instrumentos de cooperación internacional.

De manera que se entiende que, si bien no existen instrumentos de cooperación internacional específicos para hacer frente al BEC, Colombia ha participado en proyectos y programas relacionados con la prevención y el abordaje de estas amenazas, colaborando con entidades como Europol y la Fuerza de Tarea Conjunta contra el Cibercrimen. Sin embargo, aún se requieren mayores esfuerzos y suscripciones de instrumentos de cooperación para fortalecer la respuesta a este problema en el ámbito internacional.

Por otro lado, la información recopilada por medio de la entrevista efectuada a los expertos en el campo del BEC, revela aspectos relevantes que merecen un análisis exhaustivo. A continuación, se examinará detalladamente la información obtenida en respuesta a cada una de las preguntas planteadas.

En relación con la pregunta sobre las políticas formuladas en el marco de los instrumentos de cooperación internacional establecidos por Colombia en los últimos tres años para abordar las manifestaciones del BEC, se informó que hasta el momento no se han establecido políticas específicas orientadas a combatir el cibercrimen, en particular los ataques de BEC. Las actividades desarrolladas se respaldan principalmente en los Conpes 3701 de 2011 y 3854 de 2016. Aunque existe una política de seguridad digital y cibercrimen a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones, esta aborda el problema de manera holística y no se enfoca de forma precisa en el BEC.

Al cuestionar sobre el apoyo técnico establecido en el marco de los instrumentos de cooperación internacional creados por Colombia en los últimos tres años para abordar las manifestaciones del BEC, los expertos afirman que el

apoyo técnico establecido se basa, por ejemplo, en el Acuerdo Operacional de Europol, el cual permite el intercambio de experiencias y de información en la atención del fenómeno del BEC. Además, se llevan a cabo campañas de prevención e identificación de amenazas.

En la pregunta sobre las contribuciones realizadas a través de los instrumentos de cooperación internacional creados para abordar las manifestaciones del BEC, podemos entender que, a partir de sus respuestas, las contribuciones realizadas en el marco de estos instrumentos se centran en la identificación de plataformas que ofrecen servicios de *spoofing* y bloqueo de cuentas. Además, se lleva a cabo el análisis de *malware*, investigaciones conjuntas, capacitaciones y se proporciona acceso a foros de expertos.

En cuanto al tema de las instituciones que deben participar en el desarrollo de los instrumentos de cooperación internacional creados para abordar las manifestaciones del BEC, se considera fundamental, según el consenso de los expertos, la participación de todos los sectores de la sociedad en un modelo *multistakeholder*. Además, se destaca la importancia de involucrar a la academia, el sector privado, la Policía Nacional, en particular la Dijín y el Centro Cibernético Policial, la Presidencia de la República, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y otros ministerios con conocimientos sobre el tema, así como la Fiscalía General de la Nación.

En respuesta a las preguntas planteadas con relación a las funciones que deben llevar a cabo las instituciones participantes en el desarrollo de instrumentos de cooperación internacional para abordar las manifestaciones del BEC, los expertos han establecido que dichas funciones se encuentran en consonancia con lo establecido en el Conpes 3701. Cada institución, desde su misión constitucional, debe enfocarse en la prevención, atención y control del BEC. Además, es necesario describir las funciones judiciales, de investigación y de elaboración de políticas públicas para hacer frente a este fenómeno.

En cuanto a las acciones que la Policía Nacional debe emprender en materia de cooperación internacional para abordar las manifestaciones del BEC, los expertos destacan que la Institución debe enfocarse en la Estrategia Integral de Ciberseguridad de la Policía Nacional. Esto implica generar alertas, intercambiar conocimientos, referenciar expertos y compartir información relevante para enfrentar este fenómeno. También se resalta la importancia de priorizar los delitos que afectan a las pymes y mantener la cooperación con aliados estratégicos como Europol, Interpol y Eurojust.

Además, desde la perspectiva de los expertos, se han establecido acciones concretas en materia de cooperación internacional, las cuales se alinean con la Estrategia Integral de Ciberseguridad de la Policía Nacional. Estas acciones incluyen la participación en campañas de prevención y en fuerzas de tarea llevadas a cabo por Interpol y Europol. Asimismo, se recomienda fortalecer la cooperación con el sector privado, lo cual se considera una prioridad en esta materia.

El análisis de la información resalta la necesidad de que las entidades involucradas desempeñen roles definidos dentro de los acuerdos de cooperación internacional para enfrentar el BEC. Respecto a la Policía Nacional, se identifica la exigencia de implementar un conjunto diversificado de estrategias, abarcando desde la emisión de alertas y el intercambio de datos hasta el fomento de alianzas estratégicas con entidades privadas. Tales iniciativas son esenciales para combatir de manera más eficaz el BEC y para reforzar la infraestructura de seguridad digital a nivel global.

Ahora bien, en torno al cuestionario que se hizo para entender el conocimiento del comportamiento del BEC en Colombia, los resultados arrojan que, ante la pregunta sobre la modalidad de *Business Email Compromise* (BEC), se desarrolla con mayor frecuencia en el escenario internacional. La encuesta se aplicó a una muestra de 51 personas, y los resultados revelaron que el 51% de los encuestados considera que las facturas falsas son una modalidad frecuente del BEC en el ámbito internacional, mientras que el 27% las considera como la modalidad más frecuente. Asimismo, el 45% de los participantes opinó que el fraude inmobiliario se presenta con frecuencia, y el 27% lo consideró como la modalidad más frecuente. En cuanto al fraude de CEO Que consiste en la suplanta-

ción de una persona con autoridad dentro de una empresa para engañar a los empleados que tienen acceso al dinero o patrimonio de la empresa; el 41% de la población encuestada lo considera frecuente, y el 31% lo identifica como la modalidad más frecuente. Respecto a la suplantación de identidad, el 35% de los encuestados percibe su frecuencia, y el 39% señala que es la modalidad más frecuente. Por último, el robo de datos es considerado frecuente por el 24% de los participantes, mientras que el 37% lo considera más frecuente que otras modalidades, y el 27% considera que se presenta de forma demasiado frecuente.

Con respecto a la modalidad de Business Email Compromise que se desarrolla con mayor frecuencia en Colombia, de la muestra total encuestada, el 45% opina que las facturas falsas son frecuentes en Colombia, y el 27% las identifica como la modalidad más frecuente. En cuanto al fraude inmobiliario, el 41% de los participantes lo considera frecuente en el país, y el 20% lo señala como el más frecuente. Respecto al fraude de CEO, el 39% de la población encuestada lo percibe como frecuente, y el 24% lo considera el más frecuente. Ahora, sobre la suplantación de identidad, el 27% de los encuestados la considera frecuente, el 37% la identifica como más frecuente y el 20% la considera demasiado frecuente. Por último, el robo de datos es considerado frecuente por el 25% de los participantes, más frecuente por el 35% y demasiado frecuente por el 27%.

Respecto a la afirmación de que la falsificación de cuentas de correo electrónico y sitios web es una de las técnicas más utilizadas por los ciberdelincuentes para llevar a cabo el Business Email Compromise, de la muestra total, el 52.9% estuvo de acuerdo con esta afirmación, indicando que la falsificación de cuentas de correo electrónico y sitios web es una técnica ampliamente utilizada. Además, el 41.2% estuvo totalmente de acuerdo con esta afirmación. Por otro lado, el 5.9% de los encuestados manifestó su desacuerdo con dicha afirmación. Por consiguiente, esto demuestra que la percepción de los encuestados sobre las modalidades más frecuentes del Business Email Compromise en el escenario internacional y en Colombia es real y evidente; así como la importancia que tiene la falsificación de cuentas de correo electrónico y sitios web en este tipo de ataques. Estos hallazgos pueden contribuir a una mayor comprensión del problema y orientar las estrategias de prevención y respuesta ante el BEC.

Por otro lado, ante la afirmación de que el *spearphishing*, que consiste en el envío de correos electrónicos falsos, es una de las técnicas más utilizadas por los ciberdelincuentes para llevar a cabo el Business Email Compromise (BEC). Del total de la población encuestada, el 68.6% estuvo de acuerdo en que el *spearphishing* es la técnica más utilizada en esta modalidad del BEC. Además, el 23.5% estuvo totalmente de acuerdo, mientras que el 5.9% expresó su desacuerdo y el 2% estuvo en total desacuerdo con esta afirmación.

Los resultados de la investigación permiten evidenciar que el *malware*, que se refiere a programas maliciosos, es una de las técnicas más empleadas por los ciberdelincuentes para llevar a cabo el BEC. Según la población encuestada, el 60.8% estuvo de acuerdo en que el *malware* es la técnica más utilizada en estos ataques. Además, el 29.4% estuvo totalmente de acuerdo, mientras que el 9.8% expresó su desacuerdo.

En cuanto a la afirmación de que las multinacionales son las más afectadas por los ataques BEC, el 66.7% estuvo de acuerdo, mientras que el 23.5% expresó su desacuerdo y el 9.8% estuvo en total desacuerdo.

Con respecto a las empresas públicas que son las más afectadas por los ataques BEC, puede afirmarse que el 58.8% estuvo de acuerdo en que las empresas públicas son las más afectadas por los ataques BEC, mientras que el 25.5% estuvo totalmente de acuerdo y el 11.8% estuvo en desacuerdo. Por otro lado, el 3.9% estuvo totalmente en desacuerdo. En cuanto a las empresas privadas que son las más afectadas por los ataques BEC, de la población encuestada, el 68.6% estuvo de acuerdo en que las empresas privadas son afectadas por el BEC, mientras que el 21.6% estuvo en desacuerdo, el 7.8% estuvo totalmente de acuerdo y el 2% estuvo totalmente en desacuerdo.

Así se revela la percepción de la población encuestada respecto a las técnicas más utilizadas en el BEC, así como la segmentación de las empresas más afectadas según su naturaleza

(multinacionales, empresas públicas y empresas privadas). Estos datos son relevantes para comprender el panorama de los ataques BEC y pueden contribuir a la implementación de medidas de seguridad y prevención adecuadas.

Los resultados evidenciados permiten afirmar que no es posible pasar por alto las cuestiones relacionadas con los grupos delictivos organizados, ya que son los principales perpetradores de ataques BEC. De acuerdo con la población encuestada, el 56.9% está de acuerdo en que estos grupos son responsables de estos ataques, mientras que el 31.4% expresó su desacuerdo y el 11.8% estuvo totalmente de acuerdo. Esta tendencia se confirma aún más cuando consideramos que los grupos criminales organizados son quienes realizan la mayoría de los ataques BEC. Según la totalidad de la población, el 62.7% está de acuerdo en que estos grupos son los principales perpetradores de los ataques BEC, mientras que el 23.5% está en desacuerdo y el 13.7% está totalmente de acuerdo.

Frente a la afirmación de que diferentes grupos delictivos podrían estar involucrados en ataques BEC, del total de la población, el 49% estuvo de acuerdo en que estos grupos son responsables de los ataques BEC, mientras que el 41.2% expresó su desacuerdo. Además, el 7.8% estuvo totalmente de acuerdo y el 2% estuvo en total desacuerdo con esta afirmación.

Con respecto a la delincuencia organizada transnacional que realiza el mayor número de ataques BEC, según la totalidad de la población encuestada, el 62.7% estuvo de acuerdo en que la delincuencia organizada transnacional es la principal responsable de estos ataques, mientras que el 21.6% estuvo en desacuerdo. Además, el 13.7% estuvo totalmente de acuerdo y el 2% estuvo en total desacuerdo.

Frente a los delincuentes que actúan solos sin ningún tipo de nexo con organizaciones criminales o delincuenciales, del total de la población, el 56.9% está de acuerdo en que los delincuentes actúan solos sin ningún nexo con organizaciones criminales o delincuenciales, mientras que el 29.4% expresó su desacuerdo. Además, el 7.8% estuvo en total desacuerdo y el 5.9% estuvo en total acuerdo.

Lo anterior refleja la percepción de la población encuestada sobre la participación de diferentes grupos y entidades en los ataques BEC. El análisis de estas respuestas contribuye a comprender mejor la dinámica de los ataques y puede ser útil para el desarrollo de estrategias de prevención y combate efectivas.

Discusión de resultados

Con base en la información recopilada durante la ejecución del trabajo de campo, resulta relevante realizar un análisis concurrente de los resultados, tomando como puntos de enfoque los objetivos específicos establecidos en el desarrollo de la investigación. La triangulación de los hallazgos obtenidos en las fases cualitativas y cuantitativas, así como en relación con los fundamentos teóricos, permite vislumbrar los siguientes aspectos de importancia.

A escala nacional, se observa que las modalidades más frecuentes de Business Email Compromise (BEC) son la suplantación de identidad y el robo de datos, mientras que en el escenario internacional destacan las facturas falsas, el fraude inmobiliario y el fraude de suplantación CEO (engañar a los empleados de las empresas para que realicen transferencias en beneficio de los delincuentes).

Es relevante considerar que estas modalidades pueden catalogarse como comportamientos tecnológicos particulares que se manifiestan de diversas formas, debido a la amplia gama de recursos informáticos a los que se tiene acceso (Posada, 2017). Además, desde la Dirección de Investigación Criminal e Interpol, se ha observado que los ataques cibernéticos perpetrados mediante esta modalidad en el país se caracterizan por el diseño de circunstancias ficticias que engañan a los empleados, tanto de empresas públicas como privadas, mediante la suplantación de directivos o ejecutivos de las mismas. Esto conduce a la generación de fraudes empresariales mediante el robo de identidad basado en técnicas de ingeniería social (Ceballos López, 2019).

Dentro del contexto del BEC, destaca la técnica conocida como *spearphishing*. Esta estrategia se centra en el envío de correos electrónicos

o comunicaciones fraudulentas con objetivos maliciosos, que van desde el robo de datos hasta la posible instalación de malware en los dispositivos informáticos de las víctimas. Así, esta técnica aprovecha la computadora como herramienta para facilitar la comisión de delitos tradicionales que ponen en riesgo la seguridad y la tranquilidad de las personas (Temperini, 2018).

El *modus operandi* del Business Email Compromise (BEC) se caracteriza, en general, por la utilización de técnicas como correos electrónicos fraudulentos personalizados, suplantación de identidad, enmascaramiento de correos mediante el *spoofing* e infección de sitios frecuentemente visitados por empleados, también conocido como *watering hole* (Ceballos López, 2019).

Según los resultados de la encuesta, el 68.8% de la población objetivo del BEC corresponde principalmente al sector empresarial privado. En este contexto, la detección de intrusos, entendida como el uso de un sistema de detección de intrusos (IDS), desempeña un papel crucial. Un IDS es un proceso o dispositivo activo que analiza la actividad de los sistemas y redes en busca de accesos no autorizados o actividades maliciosas. Si bien los métodos de detección de anomalías pueden variar, el objetivo fundamental de cualquier IDS es detectar a los perpetradores en el momento de la acción, antes de que puedan causar daño a los recursos de la organización. Por otra parte, el sistema de confirmación se refiere a la identificación de una serie de características, rasgos e información que singularizan o destacan a un individuo, una sociedad o una organización, entre otros, contribuyendo así a la afirmación de su autenticidad.

Estas afirmaciones encuentran respaldo en el informe "El pulso del cibercrimen 2017" de Easy Solutions, que reveló que en el 2016 se crearon 13 000 nuevos sitios de *phishing* dirigidos a empresas privadas, que recibieron más de 400 000 visitas mensuales. Lo que resulta aún más alarmante es el incremento del 250% en el número de sitios de *phishing* desde el 2016. Según García (2017), el bajo costo operativo para llevar a cabo un ataque de *phishing*, combinado con la relativa facilidad técnica requerida para su ejecución, lo convierte en una estrategia sumamente atractiva para los delincuentes cibernéticos. Además, un estudio realizado por la compañía Fortinet entre abril y julio de 2019 en Colombia, reveló que se registraron más de 40 mil millones de ataques cibernéticos dirigidos al sector público y privado del país (Revista Dinero, 2019).

Ahora, los delitos asociados al BEC, se destaca la trata de personas y la explotación sexual, ya que a través de la web se facilitan los contactos y las actividades relacionadas con estas prácticas delictivas. El experto en ciberseguridad, Eddy Villanueva Díaz, enfatiza que los delitos cometidos a través de internet, especialmente en el ámbito de la trata de personas y la explotación sexual, continúan en aumento. Es preocupante la participación de menores de edad en estos casos, lo que subraya la importancia de proteger a los niños y niñas frente a posibles depredadores sexuales.

Se entiende, entonces, que el BEC se caracteriza por el empleo de estrategias sofisticadas, como la suplantación de identidad y el uso de técnicas de ingeniería social. Los sectores empresariales privados son los más afectados, y para prevenir estos delitos, se considera prioritario detectar intrusos y fortalecer los sistemas de seguridad. Además, se aboga por combatir de manera decidida la trata de personas y la explotación sexual en línea, con un enfoque especial en la protección de los menores de edad contra posibles riesgos y peligros.

Los actores ilegales que se encuentran estrechamente vinculados a esta actividad delictiva son los grupos de crimen organizado. En las últimas décadas, se ha observado un aumento significativo de las actividades ilegales llevadas a cabo por estos grupos a través de internet. Estas asociaciones criminales se caracterizan por su complejidad organizativa, operando según criterios económicos que dificultan la identificación de su carácter delictivo (Cordero, 2017).

En términos generales, la cooperación internacional frente al cibercrimen, especialmente en lo que respecta a los ataques BEC, carece de instrumentos sólidos. La Policía Nacional, junto con otras fuerzas de seguridad, participa en la tarea conjunta contra el cibercrimen. Sin embargo, en Colombia se están llevando a cabo

gestiones para formar parte del proceso enmarcado en la Convención de Cibercriminalidad. Hasta el momento, las acciones se han centrado en medidas preventivas y se trabaja en línea con el proyecto J-CAT de Europol, diseñado para hacer frente a este tipo de amenazas.

Estas acciones se explican a partir de los principios de una configuración de cooperación internacional para el desarrollo de países que deseen formar parte de dichos convenios. Para ello, la suscripción de estos acuerdos debe ser coordinada y complementaria con el propósito perseguido, como en el caso presente, la reducción de los delitos relacionados con el BEC (Prado Lallande, 2009, p. 87).

En este contexto, los programas que se desarrollan en el marco de los instrumentos de cooperación están vinculados al Centro Europeo de Cibercrimen (EC3) de Europol, que ofrece beneficios en términos de pronóstico de ataques BEC, programas de capacitación, adhesión al Convenio de Budapest y acceso a las plataformas EMAS y J-CAT para abordar este tipo de amenazas.

Esta situación está directamente relacionada con una de las múltiples formas en que se pueden establecer y suscribir convenios, en este caso, a nivel nacional e internacional con las autoridades de un país, con el fin de obtener beneficios bilaterales que contribuyan a optimizar las funciones de las organizaciones involucradas en la lucha contra el cibercrimen (Rodríguez Aguilera, 2018, p. 190).

Aunque no existen políticas específicas orientadas a abordar el cibercrimen y, en particular, los ataques BEC, hasta el momento, las actividades realizadas se apoyan en los lineamientos establecidos en los Conpes 3701 de 2011 y 3854 de 2016. Sin embargo, cabe destacar que solo se cuenta con una política de seguridad digital y cibercrimen que aborda de manera integral la problemática, pero no se enfoca específicamente en el BEC, y está a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones.

A la luz de este panorama, resulta imperativo resaltar el respaldo técnico establecido en el marco de los instrumentos de cooperación internacional. Un ejemplo destacado es el acuerdo operacional alcanzado con Europol, el cual facilita el intercambio de experiencias y de información para abordar de manera efectiva el fenómeno del cibercrimen. En adición, se llevan a cabo campañas de prevención y de identificación de amenazas. De esta manera, se puede afirmar que en Colombia la cooperación internacional se encuentra en una fase de desarrollo económico, habiendo alcanzado el límite de producción para el crecimiento de los sectores económicos y de manufactura, superando las etapas tradicionalistas e industrializadoras, y preparándose para ingresar a la etapa de consolidación basada en la tecnología (Slater, 1999).

Con relación a las contribuciones realizadas en el marco de los instrumentos de cooperación internacional, resulta relevante destacar los esfuerzos dirigidos a la identificación de plataformas que ofrecen servicios como el *spoofing* y el bloqueo de cuentas. Asimismo, se llevan a cabo análisis de malware, investigaciones conjuntas, programas de capacitación y se fomenta el acceso a foros de expertos.

De igual manera, la Policía Nacional debe articularse con todos los sectores de la sociedad y adoptar un enfoque de múltiples partes interesadas (*multistakeholder*), incluyendo la academia y el sector privado. En este sentido, la Policía Nacional, por medio de la Dirección de Investigación Criminal e Interpol y su Centro Cibernético Policial, debe establecer una sinergia directa y completa con la Presidencia de la República, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y otros ministerios involucrados en el tema, así como con la Fiscalía General de la Nación.

Además, en el desarrollo de esta simbiosis, tanto la Policía Nacional como las demás instituciones involucradas deben cumplir con lo establecido en el Conpes 3701. Cada institución, desde su misión constitucional, tiene la capacidad y la responsabilidad de dedicarse a la prevención, atención y control del cibercrimen. Asimismo, resulta necesario describir las funciones judiciales relacionadas con la investigación y la formulación de políticas públicas.

Por último, es fundamental que la Policía Nacional lleve a cabo acciones concretas en concordancia con la Estrategia Integral de Ciberseguridad

ridad. Esto implica generar alertas, fomentar el intercambio de conocimiento, establecer referencias a expertos y promover el intercambio de información para enfrentar eficazmente el fenómeno del cibercrimen. Asimismo, se debe priorizar la atención a los delitos que impactan la economía de las pymes, sin descuidar la cooperación con los aliados estratégicos como Europol, Interpol y Eurojust.

Conclusiones

Después de examinar los resultados obtenidos durante el trabajo de campo, se concluye que, a nivel nacional, la tipología recurrente del Business Email Compromise (BEC) está relacionada principalmente con la infiltración de correos electrónicos corporativos. La suplantación de identidad y el robo de datos son los métodos más frecuentes utilizados para tal fin. En el ámbito internacional, se identifican como acciones recurrentes en el BEC la emisión de facturas falsas, el fraude inmobiliario y el fraude CEO, que implica engañar a los empleados de una empresa para que realicen transferencias en beneficio de los estafadores. Estas manifestaciones del BEC delinean un panorama claro de la amenaza cibernética más impactante en el país.

Los actores más susceptibles de ser afectados por estas formas de BEC, en orden de importancia, son los organismos multinacionales, las empresas privadas y las empresas públicas. En términos de asociación delictiva, el BEC guarda una relación prioritaria con la trata de personas, la explotación sexual, el narcotráfico y el tráfico de órganos. Cabe destacar que el BEC presenta una mayor vinculación con los grupos criminales organizados que con los grupos delictivos organizados, siendo la delincuencia organizada transnacional la que lleva a cabo la mayoría de los ataques cibernéticos bajo esta modalidad.

La falta de instrumentos de cooperación específicos para abordar el cibercrimen, particularmente los ataques BEC, es evidente. La Policía Nacional, en colaboración con otras fuerzas de seguridad, participa en la tarea conjunta contra el cibercrimen. En Colombia, se están llevando a cabo gestiones para formar parte del proceso que se enmarca en la Convención de Cibercriminalidad. Hasta el momento, las actividades se centran en la prevención y se alinean con el proyecto J-CAT de Europol, diseñado para abordar estas amenazas.

Los programas en curso en el marco de los instrumentos de cooperación se relacionan con el EC3 de Europol, que ofrece capacidades de pronóstico de ataques BEC, así como programas de capacitación, participación en el Convenio de Budapest y acceso a las plataformas EMAS y J-CAT para abordar estas amenazas. Aunque no existen políticas específicas para abordar el cibercrimen y, en particular, los ataques BEC, las actividades hasta ahora se respaldan en los lineamientos establecidos en los Conpes 3701 de 2011 y 3854 de 2016. Si bien existe una política integral de seguridad digital y cibercrimen a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones, esta no aborda directamente el BEC. En este contexto, surge la necesidad de respaldar las propuestas acordadas con otros países interesados en la cooperación, así como promover la transferencia tecnológica para lograr un desarrollo tangible más significativo (Brofman & Díaz Polanco, 2003, p. 236).

Finalmente, la comisión permanente del servicio en el exterior de Europol ha implementado las plataformas digitales EMAS y J-CAT, que se centran en investigaciones conjuntas, soporte técnico y forense, así como capacitación. Esta iniciativa puede formar parte integral de las estrategias de cooperación integral mediante la firma de instrumentos de cooperación internacionales. Un importante descubrimiento derivado de la investigación es la falta de una política específica para abordar las modalidades del cibercrimen. Si bien los últimos Conpes 3701 y 3854 hacen referencia a una política estatal sobre el cibercrimen y la seguridad digital de los ciudadanos colombianos, estos documentos también reconocen que actualmente "el Estado colombiano carece de la capacidad para anticipar y prevenir cualquier tipo de amenaza cibernética o digital". Por tanto, se considera de gran importancia fortalecer la cooperación con el sector privado, lo cual debe ser una prioridad tanto nacional como internacional.

Además de lo descrito, pueden vislumbrarse algunos aspectos considerados como proyección de esta investigación:

Dada la creciente incidencia de amenazas cibernéticas, como el Business Email Compromise (BEC), es imprescindible proponer respuestas coordinadas en el escenario internacional basadas en un modelo de cooperación internacional policial desarrollado en Colombia. Este modelo ha demostrado su eficacia en el contexto colombiano; además de ofrecer un enfoque global e integral que puede adaptarse y adoptarse a nivel mundial. En este documento, además, se ha establecido un plan de acción que prevé la implementación y adaptación de este modelo en tres etapas: corto plazo (2024), mediano plazo (2027) y largo plazo (2030). Cada fase se centrará en aumentar la capacidad de respuesta frente a las amenazas cibernéticas, adaptándose a los avances de la cuarta revolución industrial, y proporcionando una herramienta esencial para los Estados en su lucha continua por garantizar la seguridad cibernética.

Fases del modelo

Corto plazo (2024). En esta fase inicial, se establecen dos actividades clave. La primera es la "Sensibilización y capacitación", que tiene como objetivo principal aumentar la conciencia sobre las amenazas cibernéticas, con un enfoque específico en el BEC. Además, se busca fortalecer la educación de los actores clave tanto en los sectores público como privado. Esto incluye la promoción de la formación especializada de agentes de la ley y funcionarios de seguridad para enfrentar estos desafíos. La segunda actividad es la "Creación de redes y colaboración", que se enfoca en fomentar el establecimiento y fortalecimiento de redes entre las organizaciones de aplicación de la ley a nivel nacional e internacional. Uno de los objetivos prioritarios aquí es desarrollar mecanismos sólidos de intercambio de información y cooperación.

Mediano plazo (2027). En esta etapa intermedia, se plantean dos objetivos significativos. El primero es la "Adaptación y adopción de tecnologías avanzadas", que implica la incorporación de tecnologías de vanguardia, como la inteligencia artificial, Big Data y el aprendizaje automático. Estas tecnologías se utilizan para identificar y prevenir amenazas cibernéticas, incluido el BEC. El segundo objetivo es la "Ley y regulación", que se centra en revisar y actualizar las leyes y regulaciones existentes para que sean adecuadas al entorno cibernético en constante cambio. La cooperación internacional desempeñará un papel fundamental en este esfuerzo.

Largo plazo (2030). En la fase a largo plazo, se establecen dos metas principales. La primera es "Innovación continua", que busca mantenerse al día con las tácticas cambiantes de los delincuentes cibernéticos a medida que evolucionan las amenazas cibernéticas. Esto requerirá una inversión sostenida en investigación y desarrollo (I+D), así como una cultura de aprendizaje y adaptación constante. La segunda meta es la "Integración global y estrategias a largo plazo", que aspira a establecer una red global sólida de cooperación policial en el ciberespacio. Las estrategias a largo plazo se enfocarán en mantener y fortalecer esta red y en trabajar de manera continua para integrar y coordinar las estrategias de lucha contra el ciberdelito en el escenario internacional.

En cuanto a los resultados previstos y la evaluación de la efectividad de la cooperación internacional policial, se llevará a cabo a través de indicadores específicos. Estos indicadores pueden incluir la reducción en la incidencia de amenazas cibernéticas como el BEC, el aumento en la capacitación del personal de seguridad en ciberseguridad y la efectividad de las acciones de cooperación policial. Un resultado esperado de vital importancia será la firma de un memorando de entendimiento entre las partes involucradas, que establecerá un marco formal para la cooperación en este ámbito. El respaldo de organismos multilaterales, como la ONU, será fundamental para reforzar la legitimidad y eficacia de estas acciones.

Resultados esperados y medición del impacto

La efectividad de la cooperación internacional policial se traduciría en una serie de resultados concretos que tienen un impacto directo en la seguridad cibernética. Entre los resultados que se esperarían con su implementación se incluyen:

Reducción de la incidencia de amenazas cibernéticas: se anticipa que la cooperación internacional conduciría a una disminución en la incidencia de amenazas cibernéticas, como el BEC. Esto significa que habría menos ataques cibernéticos y menos víctimas de estos delitos.

Aumento de la capacitación en ciberseguridad: el número de profesionales de seguridad capacitados en ciberseguridad aumentaría significativamente. Esto se traduciría en una fuerza laboral mejor preparada para prevenir y responder a las amenazas cibernéticas.

Mayor efectividad en las acciones de cooperación policial: la colaboración entre las fuerzas de seguridad en el ámbito internacional sería más efectiva. Esto permitiría una respuesta más rápida y coordinada ante los delincuentes cibernéticos, lo que a su vez reduciría el impacto de sus actividades.

Firma de un memorando de entendimiento: un resultado crucial sería la firma de un memorando de entendimiento entre las partes involucradas. Esto establecería un marco formal para la cooperación en ciberseguridad, lo que facilitaría aún más la colaboración y el intercambio de información.

En cuanto a la identificación de desafíos y limitaciones, se anticipa que estos podrían abordar cuestiones de capacidad, como la necesidad de desarrollar habilidades técnicas y conocimientos específicos en ciberseguridad entre el personal de seguridad. Además, podrían surgir desafíos legales relacionados con la necesidad de alinear las leyes y regulaciones con la evolución constante de las amenazas cibernéticas. Asimismo, la disponibilidad de recursos financieros puede representar una posible limitación.

Para superar estos desafíos y garantizar una implementación efectiva del proyecto, se requerirá un enfoque estratégico desde el inicio. Identificar y desarrollar estrategias sólidas que aborden cada uno de estos desafíos será crucial para asegurar el éxito del proyecto.

Un futuro de cooperación internacional

En el marco de este plan de acción, la propuesta de un modelo de cooperación internacional policial, basado en una rigurosa investigación académica, se presenta como una iniciativa pionera. Este modelo tiene el potencial de revolucionar la forma en que enfrentamos las amenazas cibernéticas en un mundo cada vez más interconectado.

Se reconoce que, debido a la naturaleza dinámica del ciberespacio y la rápida evolución de las amenazas cibernéticas, se requerirá un proceso de revisión y actualización continua del plan de acción y sus estrategias. Este proceso podría establecerse en un ciclo anual, con la posibilidad de revisiones más frecuentes si la situación lo requiere. La cooperación y el intercambio de información entre todas las partes involucradas serán fundamentales para esta revisión y actualización continua.

En este contexto, la visión subyacente de este modelo es la de un mundo digital más seguro, donde los Estados trabajan juntos, compartiendo recursos y conocimientos para proteger a sus ciudadanos y al ciberespacio global de amenazas emergentes. Una vez implementado, este modelo tiene el potencial de convertirse en una herramienta invaluable para prevenir y mitigar las amenazas cibernéticas, no solo en Colombia, sino también en todo el mundo

En este mismo sentido, es necesario tener en cuenta las siguientes recomendaciones dentro de la proyección: (a) Fomentar la participación de todas las partes interesadas: asegurar que todos los actores relevantes, incluyendo gobiernos, organismos internacionales y sector privado estén involucrados y comprometidos con el proceso desde su inicio, promoviendo así una cooperación eficaz y sostenible; (b) Capacitación continua y actualización de habilidades: dado que el panorama de las amenazas cibernéticas está en constante evolución, es crucial que se implementen programas de formación continua para mantener a las fuerzas de seguridad al día con las últimas tácticas, técnicas y procedimientos en ciberseguridad. (3) Desarrollar y mantener un marco legal sólido: asegurarse de que existe un marco legal claro y actualizado que apoye y facilite la cooperación internacional en la lucha contra las amenazas cibernéticas, y que este se revise y actualice constantemente para mantenerse alineado con las cambiantes dinámicas del ciberespacio.

Referencias

Aguirre García, J. C., & Jaramillo Echeverri, L. G. (2012). Aportes del método fenomenológico a la investigación cualitativa. *Revista Latinoamericana de Estudios Educativos*, *8*(2) 51-74.

Álvarez, R. (2019). *Jonathan James, el joven que con sólo 15 años hackeó y puso de cabeza a la NASA y al Pentágono*. Xataka. https://acortar.link/cJILUW

Bisquerra, R. (2009). *Metodología de la investigación cualitativa*. La Muralla. S.A.

Brofman, M., & Díaz Polanco, J. (2003). La cooperación técnica internacional y las políticas de salud. *Ciencia & Saude Colectiva*, 8(1), 227-242.

Ceballos López, A. (2019). *Informe de las tendencias cibercrimen Colombia 2019-2020*. Dirección de Investigación Criminal e Interpol.

Colprensa. (2019, julio 21). Colombia fue uno de los países con más ataques cibernéticos el año pasado. *Colprensa*. https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. (CONPES). (2020). Documento Conpes 3995 Política Nacional de Confianza y Seguridad Digital.

Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. (CONPES). (2011, julio) Documento Conpes 3701 Lineamientos de política para ciberseguridad y ciberdefensa.

Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. (CONPES). (2016, abril) Documento Conpes 3854 Política nacional de seguridad digital.

Cordero, R., & Salinas, F. (2017). Hacia una sociología de la abstracción: observaciones acerca de la mediación entre lo conceptual y lo empírico. *Cinta Moebio Revista Electrónica de Epistemología de las Ciencias Sociales, 58, 61-73.* https://doi.org/10.4067/S0717-554X2017000100061

Creswell, J. W. (2008). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (3rd ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Duarte Herrera, L. K., & González Parias, C. H. (2014). Origen y evolución de la cooperación internacional para el desarrollo. *Panorama, 8*(15), 117-131. https://doi.org/10.15765/pnrm.v8i15.554

Deutsche Welle (DW). (2019). *Seis ataques cibernéticos que sacudieron el mundo*. https://acortar.link/ffRXEf

García, M. C. (2017, octubre 1*). El salto de Easy Solutions a las grandes ligas de la tecnología*. Diario El Tiempo. https://www.eltiempo.com/economia/empresas/easy-solutions-empresa-se-soluciones-contra-el-fraude-electronico-275254

Hernández, R. Fernández, C., & Baptista, L. (2010). Metodología de la investigación. En R. Hernández Sampieri. *Los métodos mixtos* (pp. 546-601). McGraw-Hill.

Hernández, R. Fernández, C., & Baptista, L. (2014). *Metodología de la investigación*. McGraw-Hill.

Jiménez González, C. (2003). Las teorías de la cooperación internacional dentro de las relaciones internacionales. *Investigación y Análisis Sociopolítico y Psicosocial*, 2(3), 115 – 147.

Navarro Asencio, E., Jiménez, E., Rappoport, S., & Thoilliez, B. (2017). *Fundamentos de la investigación e innovación educativa*. Universidad Internacional de la Rioja (UNIR).

Oliveira, J. (2017, mayo 15). El ataque de 'ransomware' se extiende a escala global. *El País*.

https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html

Otero, C. (2019, enero 4). *Alemania hackeada: roban y filtran los datos de Angela Merkel y otros 1000 políticos*. Betech. https://as.com/meristation/2019/01/04/betech/1546603858_337341.html

Pérez Serrano, G. (1994). *Investigación cualitativa retos e interrogante*. La Muralla S. A.

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo Foro Penal*, *13*(88), 72-112.

Prado Lallande, J. P. (2009). El impacto de la cooperación internacional en el desarrollo de la democracia y los derechos humanos. *Perfiles Latinoamericanos*, *17*(33), 65-93. https://doi.org/10.18504/pl1733-065-2009

Ramírez, M. C. (2019, junio 28). *El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia.* La República. https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

Rayon, T., Menchero, S., Nieto, A., Xenopoulos, P., Crespo, M., Cockburn, K., Cañon, S., Sasaki, H., Hadjantonakis, A.K., de la Pompa, J. L., Rossant, J., & Manzanares, M. (2014). Notch and hippo converge on Cdx2 to specify the trophectoderm lineage in the mouse blastocyst. *Developmental Cell, 30*(4), 410-422. https://doi.org/10.1016/j.devcel.2014.06.019

Restrepo Silva, M. (2012). La cooperación internacional al desarrollo como herramienta de protección y promoción de los derechos humanos. Caso latinoamericano. *Revista Facultad de Derecho y Ciencias Políticas*, *42*(116), 271-295.

Reveles L. R. (2019). *Análisis de los elementos del costo*. IMCP. Instituto Mexicano de Contadores Públicos. México.

Revista Dinero. (2019, mayo 9). *En solo tres meses Colombia sufrió 42 billones de intentos de atentados terroristas*. Revista Dinero. https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

Rocco, T. (2003). Taking the next step: Mixed methods research in organizational systems. *Information Technology, Learning, and Performance Journal, 21*(1), 19-29.

Rodríguez Aguilera, C. L. (2018). El modelo de cooperación de la comunidad andina en materia migratoria. *Revista De La Secretaría Del Tribunal Permanente De Revisión, 6*(11), 175-192. https://doi.org/10.16890/rstpr.a6.n11.p175

Slater, F. (1999). *Las etapas de crecimiento económico de Rostow. Consideraciones del evolucionismo como modelo interpretativo*. *Soñando el Sur*, (2), 114-121. https://repositoriodigital.uct.cl/handle/10925/302.

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. En *Ciber crimen y delitos informáticos* (pp. 39-68). Erreirus.

Virtualpro. (2019, enero 4). *Colombia ocupa el cuarto lugar de países con más víctimas de ciberataques.* Virtualpro. https://www.virtualpro.co/noticias/colombia-ocupa-el-cuarto-lugar-de-paises-con-mas-victimas-de-ciberataques

Anexos

Anexo 1.

POLICÍA NACIONAL DE COLOMBIA
DIRECCIÓN NACIONAL DE ESCUELAS
ESCUELA DE POSTGRADOS DE POLICÍA "MIGUEL ANTONIO LLERAS PIZARRO"
MAESTRÍA EN SEGURIDAD PÚBLICA MASEP XIV

Objetivo. Caracterizar la amenaza cibernética hurto por medios informáticos en la modalidad BEC (Bussiness Email Compromise) presente en el país.

Factor Identificación

Edad (años) _____ Sexo: F____ M_____ Profesión Empleado Público___ Independiente _____ Empresario _____Otro. ¿Cuál? _____

Factor Modalidades

En una escala de 1 a 5 (donde 1 es menos frecuente y 5 más frecuente), ¿cuál considera Usted que es la modalidad de Bussiness Email Compromise que se desarrolla con más frecuencia a nivel internacional?

Facturas falsas

Suplantación de identidad

Fraude del CEO

Robo de datos

Fraude inmobiliario

Otro. ¿Cuál? _____

En una escala de 1 a 5 (donde 1 es menos frecuente y 5 más frecuente), ¿cuál considera usted que es la modalidad del Bussiness Email Compromise que se desarrolla con más frecuencia en Colombia?

Facturas falsas

Suplantación de identidad

Fraude del CEO (Chief Executive Officer)

Robo de datos

Fraude inmobiliario

Otro. ¿Cuál? _____

Factor Técnicas

A continuación, encontrará una serie de afirmaciones que deben ser valoradas por usted con la siguiente escala Likert

TA	A	D	TD
Total Acuerdo	Acuerdo	Desacuerdo	Total Desacuerdo

TÉCNICAS EMPLEADAS POR HACKERS	TA	A	TD	D
La falsificación de cuentas de correo electrónico y sitios web es una de las técnicas más utilizadas por los hackers para llevar a cabo ***Bussiness Email Compromise***.				
El ***spear-phishing*** **(correos electrónicos falsos)** es una de las técnicas más utilizadas por los hackers para llevar a cabo Bussiness Email Compromise.				
El ***malware*** **(programa malicioso)** es una de las técnicas más utilizadas por los hackers para llevar a cabo Bussiness Email Compromise.				
Otro. ¿Cuál?				

Factor Población Objetivo

POBLACIÓN OBJETIVO ATAQUES BEC	TA	A	TD	D
Las multinacionales son las más afectadas por ataques BEC				
¿De cuál actividad económica?				
Las empresas públicas son las más afectadas por ataques BEC				
¿De cuál actividad económica?				
Las empresas privadas son las más afectadas por ataques BEC				
¿De cuál actividad económica?				
Las personas naturales son las más afectadas por ataques BEC				
¿De qué tipo de trabajo?				

Factor Asociación

ASOCIACIÓN A OTROS DELITOS	TA	A	TD	D
La venta ilegal de armas es el delito que tiene mayores casos de asociación con el desarrollo de ataques BEC				
El narcotráfico es el delito que tiene mayores casos de asociación con el desarrollo de ataques BEC				
La trata de personas es el delito que tiene mayores casos de asociación con el desarrollo de ataques BEC				
La explotación sexual es el delito que tiene mayores casos de asociación con el desarrollo de ataques BEC				
El tráfico de órganos es el delito que tiene mayores casos de asociación con el desarrollo de ataques BEC				
Otro. ¿Cuál?				

Factor Actores Ilegales

ACTORES ILEGALES BEC	TA	A	TD	D
Los Grupos Delictivos Organizados son quienes realizan el mayor número de ataques BEC				
Los Grupos Criminales Organizados son quienes realizan el mayor número de ataques BEC				
Los Grupos Armados Organizados son quienes realizan el mayor número de ataques BEC				
Las disidencias son quienes realizan el mayor número de ataques BEC				
La delincuencia organizada transnacional realiza el mayor número de ataques BEC				
Los delincuentes actúan solos sin ningún tipo de nexo con organizaciones criminales o delincuenciales				
Otro. ¿Cuál?				

Factor Acciones De Defensa

ACCIONES DE DEFENSA PARA ATAQUES BEC	TA	A	TD	D
Sistema de detección de intrusos a través de correos electrónicos que se señalan con extensiones que son similares al correo electrónico de la empresa.				
Codificación de colores para la identificación de correos electrónicos de las cuentas internas de los empleados para diferenciarlos de los correos electrónicos de las cuentas externas.				
Solicitudes de confirmación para transferencias de fondos con verificación telefónica como parte de un esquema de autenticación de factores.				
Bloqueo de correos electrónicos fraudulentos implementando técnicas de validación de origen de mensaje.				
Capacitación periódica de los usuarios sobre la importancia de la seguridad con un enfoque centrado en las personas para combatir los ataques de correo electrónico.				
Otro. ¿Cuál?				

Factor Actores Legales

ACTORES DEFENSA PARA ATAQUES BEC	TA	A	TD	D
El Gobierno a través de su institucionalidad ha desarrollado estrategias para contrarrestar las acciones BEC				
¿Qué instituciones?				
¿Cuáles estrategias?				
La fuerza pública ha desarrollado estrategias para contrarrestar las acciones BEC				
¿Qué instituciones?				
¿Cuáles estrategias?				
Organismos y/o actores internacionales han desarrollado estrategias para afrontar los efectos BEC				
¿Qué instituciones?				
¿Cuáles estrategias?, a través de qué tipo de cooperación (bilateral, triangular o multilateral)				

Anexo 2

POLICÍA NACIONAL DE COLOMBIA
DIRECCIÓN NACIONAL DE ESCUELAS
ESCUELA DE POSTGRADOS DE POLICÍA "MIGUEL ANTONIO LLERAS PIZARRO"
MAESTRÍA EN SEGURIDAD PÚBLICA MASEP XIV

Objetivo. Describir los instrumentos de cooperación internacional policial suscritos en los tres últimos años por Colombia, así como las acciones que la Policía Nacional de Colombia en materia de cooperación internacional policial debería aplicar para hacer frente a esta amenaza cibernética que afecta la seguridad pública.

Tipología

1. ¿De qué tipo han sido los instrumentos de cooperación interinstitucional que Colombia ha creado a nivel internacional en los últimos tres años en torno a la atención de las manifestaciones del Bussiness Email Compromise?

Proyectos

2. ¿Cuáles son los proyectos que se adelantan en el marco de los instrumentos de cooperación que Colombia ha creado a nivel internacional en los últimos tres años en torno a la atención de las manifestaciones del Bussiness Email Compromise?

3. ¿Cuáles han sido los programas que se adelantan en el marco de los instrumentos de cooperación que Colombia ha creado a nivel internacional en los últimos tres años en torno a la atención de las manifestaciones del Bussiness Email Compromise?

4. ¿Qué políticas se han formulado en el marco de los instrumentos de cooperación que Colombia ha creado a nivel internacional en los últimos tres años en torno a la atención de las manifestaciones del Bussiness Email Compromise?

Apoyos Técnicos

5. ¿Cuál ha sido el apoyo técnico (envío de expertos, actividades de investigación, contratos de servicios) que se ha establecido en el marco de los instrumentos de cooperación internacional que ha creado en los últimos tres años en torno a la atención de las manifestaciones del Bussiness Email Compromise?

Contribuciones

6. ¿Qué tipo de contribuciones se han llevado a cabo a través de los instrumentos de cooperación internacional que se han creado en torno a la atención de las manifestaciones del Bussiness Email Compromise?

Actores

7. ¿Qué instituciones deben participar en el desarrollo de los instrumentos de cooperación internacional que se han creado en torno a la atención de las manifestaciones del Bussiness Email Compromise?

8. ¿Qué funciones deben adelantar las instituciones que participan en el desarrollo de instrumentos de cooperación internacional que se han creado en torno a la atención de las manifestaciones del Bussiness Email Compromise?

Estrategia

9. ¿A quiénes debe convocar la Policía Nacional en materia de cooperación internacional para la atención de las manifestaciones del Bussiness Email Compromise?

10. ¿Qué acciones debe adelantar la Policía Nacional en materia de cooperación internacional para la atención de las manifestaciones del Bussiness Email Compromise?

11. ¿Cómo debe adelantar la Policía Nacional las acciones establecidas en materia de cooperación internacional para la atención de las manifestaciones del Bussiness Email Compromise?